ON THE ARITY GAP OF POLYNOMIAL FUNCTIONS

MIGUEL COUCEIRO, ERKKO LEHTONEN, AND TAMÁS WALDHAUSER

Abstract. The authors' previous results on the arity gap of functions of several variables are refined by considering polynomial functions over arbitrary fields. We explicitly describe the polynomial functions with arity gap at least 3, as well as the polynomial functions with arity gap equal to 2 for fields of characteristic 0 and finite fields of characteristic 2. These descriptions are given in the form of decomposition schemes of polynomial functions.

1. Introduction and preliminaries

Throughout this section, let A and B be arbitrary sets with at least two elements. A *partial function of several variables* from A to B is a mapping $f\colon S \to B$, where $S \subseteq A^n$ for some integer $n \geq 1$, called the *arity* of f. If $S = A^n$, then we speak of (*total*) *functions of several variables.* Functions of several variables from A to A are referred to as *operations* on A.

For an integer $n \geq 1$, let $[n] := \{1, \ldots, n\}$. Let $f\colon S \to B$ ($S \subseteq A^n$) be an n-ary partial function and let $i \in [n]$. We say that the i-th variable is *essential* in f (or f *depends* on x_i), if there exist tuples

$$(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n), (a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n) \in S$$

such that

$$f(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n).$$

Variables that are not essential are called *inessential.* Let $\operatorname{Ess} f := \{i \in [n] : x_i \text{ is essential in } f\}$. The cardinality of $\operatorname{Ess} f$ is called the *essential arity* of f and denoted by $\operatorname{ess} f$.

Let $f\colon A^n \to B$, $g\colon A^m \to B$. We say that g is a *simple minor* of f, if there is a map $\sigma\colon [n] \to [m]$ such that $g(x_1, \ldots, x_m) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. We say that f and g are *equivalent* if each one is a simple minor of the other.

For $i, j \in [n]$, $i \neq j$, define the *identification minor* of $f\colon A^n \to B$ obtained by identifying the i-th and the j-th variable, as the simple minor $f_{i \leftarrow j}\colon A^n \to B$ of f corresponding to the map $\sigma\colon [n] \to [n]$, $i \mapsto j$, $\ell \mapsto \ell$ for $\ell \neq i$, i.e., $f_{i \leftarrow j}$ is given by the rule

$$f_{i \leftarrow j}(x_1, \ldots, x_n) := f(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_n).$$

Remark 1.1. Loosely speaking, a function g is a simple minor of f, if g can be obtained from f by permutation of variables, addition of inessential variables and identification of variables. Similarly, two functions are equivalent, if one can be obtained from the other by permutation of variables and addition of inessential variables.

The *arity gap* of f is defined as

$$\operatorname{gap} f := \min_{\substack{i,j \in \operatorname{Ess} f \\ i \neq j}} (\operatorname{ess} f - \operatorname{ess} f_{i \leftarrow j}).$$

Remark 1.2. Note that the definition of arity gap refers only to essential variables. Hence, in order to determine the arity gap of a function f, we may consider instead an equivalent function f' that is obtained from f by removing its inessential variables. It is easy to see that $\operatorname{gap} f = \operatorname{gap} f'$. Therefore, whenever we consider the arity gap of a function f, we may assume without loss of generality that f depends on all of its variables.

Example 1.3. Let F be an arbitrary field. Consider the polynomial function $f\colon F^3 \to F$ induced by $x_1x_3 - x_2x_3$. It is clear that all variables of f are essential, i.e., $\operatorname{ess} f = 3$. Let us form the various identification minors of f:

$$\begin{aligned} f_{1\leftarrow 2} &= 0, & f_{2\leftarrow 1} &= 0, \\ f_{1\leftarrow 3} &= x_3^2 - x_2x_3, & f_{3\leftarrow 1} &= x_1^2 - x_1x_2, \\ f_{2\leftarrow 3} &= x_1x_3 - x_3^2, & f_{3\leftarrow 2} &= x_1x_2 - x_2^2. \end{aligned}$$

The essential arities of the identification minors are

$$\begin{aligned} &\operatorname{ess} f_{1\leftarrow 2} = \operatorname{ess} f_{2\leftarrow 1} = 0, \\ &\operatorname{ess} f_{1\leftarrow 3} = \operatorname{ess} f_{3\leftarrow 1} = \operatorname{ess} f_{2\leftarrow 3} = \operatorname{ess} f_{3\leftarrow 2} = 2. \end{aligned}$$

We conclude that $\operatorname{gap} f = 1$.

Example 1.4. Let $f\colon \{0,1\}^n \to \{0,1\}$ $(n \geq 2)$ be the function induced by the polynomial $x_1 + x_2 + \cdots + x_n + c$ $(c \in \{0,1\})$ over the two-element field. Then for each $i \neq j$ we have that $f_{i\leftarrow j}$ is induced by the polynomial

$$\Big(\sum_{\ell \in [n] \setminus \{i,j\}} x_\ell \Big) + c.$$

Thus $\operatorname{ess} f = n$ and $\operatorname{ess} f_{i\leftarrow j} = n-2$ for all $i \neq j$; hence $\operatorname{gap} f = 2$. It was shown by Salomaa [8] that every operation on $\{0,1\}$ has arity gap at most 2. The operations on $\{0,1\}$ were classified according to their arity gap in [2], where it was shown that for $n \geq 4$, the linear functions mentioned above are the only operations on $\{0,1\}$ that have essential arity n and arity gap equal to 2.

Example 1.5. Let A be a finite set with $k \geq 2$ elements, say, $A = \{0, 1, \ldots, k-1\}$. Let $f\colon A^n \to A$, $2 \leq n \leq k$, be given by the rule

$$f(a_1, \ldots, a_n) := \begin{cases} 1 & \text{if } (a_1, \ldots, a_n) = (0, 1, \ldots, n-1), \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that all variables of f are essential, and for all $i \neq j$, the function $f_{i\leftarrow j}$ is identically 0. Hence $\operatorname{gap} f = n$. This example illustrates the fact that there exist functions of arbitrarily high arity gap.

The notion of arity gap has been studied by several authors [2, 3, 4, 5, 6, 7, 8, 9, 10]. In [3], a general classification of functions according to their arity gap was established. In order to state this result, we need to recall a few notions.

For $n \geq 2$, define

$$A^n_{=} := \{(a_1, \ldots, a_n) \in A^n : a_i = a_j \text{ for some } i \neq j\}.$$

Furthermore, define $A^1_{=} := A$. Let $f\colon A^n \to B$. Any function $g\colon A^n \to B$ satisfying $f|_{A^n_{=}} = g|_{A^n_{=}}$ is called a *support* of f. The *quasi-arity* of f, denoted $\operatorname{qa} f$, is defined as the minimum of the essential arities of all supports of f, i.e., $\operatorname{qa} f := \min_g \operatorname{ess} g$ where g ranges over the set of all supports of f. If $\operatorname{qa} f = m$, then we say that f is *quasi-m-ary*. Note that if A is finite and $n > |A|$, then $A^n_{=} = A^n$; hence $\operatorname{qa} f = \operatorname{ess} f$. Moreover, $\operatorname{qa} f = \operatorname{ess} f|_{A^n_{=}}$ whenever $n \neq 2$.

Denote by $\mathcal{P}(A)$ the power set of A, and define the function $\operatorname{oddsupp}\colon \bigcup_{n\geq 1} A^n \to \mathcal{P}(A)$ by

$$\operatorname{oddsupp}(a_1, \dots, a_n) := \{a \in A : |\{j \in [n] : a_j = a\}| \text{ is odd}\}.$$

We say that a partial function $f\colon S \to B$ ($S \subseteq A^n$) is *determined by* oddsupp if there exists a function $f^*\colon \mathcal{P}(A) \to B$ such that

$$f = f^* \circ \operatorname{oddsupp}|_S. \tag{1}$$

Observe that only the restriction of f^* to the set

$$\mathcal{P}'_n(A) := \big\{S \in \mathcal{P}(A) : |S| \in \{n, n-2, n-4, \dots\}\big\},$$

is relevant in determining the values of f in (1). Moreover, the functions $f\colon A^n \to B$ determined by oddsupp are in one-to-one correspondence with the functions $f^*\colon \mathcal{P}'_n(A) \to B$.

The notion of a function being determined by oddsupp is due to Berman and Kisielewicz [1]. Willard showed in [10] that if $f\colon A^n \to B$, where A is finite, $\operatorname{ess} f = n > \max(|A|, 3)$ and $\operatorname{gap} f \geq 2$, then f is determined by oddsupp. The following fact is easy to verify.

Fact 1.6. *A function $f\colon A^n \to B$ is determined by* oddsupp *if and only if f is totally symmetric and $f_{2\leftarrow 1}$ does not depend on x_1.*

We can now state the general classification of functions according to the arity gap. This result was first obtained in [3] for functions with finite domains, and in [5] it was shown to still hold for functions with arbitrary, possibly infinite domains.

Theorem 1.7. *Let A and B be arbitrary sets with at least two elements. Suppose that $f\colon A^n \to B$, $n \geq 2$, depends on all of its variables.*

(i) *For $3 \leq p \leq n$, $\operatorname{gap} f = p$ if and only if $\operatorname{qa} f = n - p$.*

(ii) *For $n \neq 3$, $\operatorname{gap} f = 2$ if and only if $\operatorname{qa} f = n - 2$ or $\operatorname{qa} f = n$ and $f|_{A^n_{=}}$ is determined by* oddsupp.

(iii) *For $n = 3$, $\operatorname{gap} f = 2$ if and only if there is a nonconstant unary function $h\colon A \to B$ and $i_1, i_2, i_3 \in \{0, 1\}$ such that*

$$f(x_1, x_0, x_0) = h(x_{i_1}),$$
$$f(x_0, x_1, x_0) = h(x_{i_2}),$$
$$f(x_0, x_0, x_1) = h(x_{i_3}).$$

(iv) *Otherwise $\operatorname{gap} f = 1$.*

Theorem 1.7 can be refined to obtain more explicit classifications by assuming certain structures on the domain A or the codomain B of f. Examples of such refinements include the complete classification of Boolean functions [2], pseudo-Boolean functions [3], lattice polynomial functions [4], or more generally, order-preserving functions [6]. Moreover, in [5], B was assumed to be a group, and the following decomposition scheme based on the quasi-arity was obtained.

Theorem 1.8. *Assume that $(B;+)$ is a group with neutral element 0. Let $f\colon A^n \to B$, $n \geq 3$, and $1 \leq p \leq n$. Then the following two conditions are equivalent:*

(i) $\operatorname{ess} f = n$ *and* $\operatorname{qa} f = n - p$.

(ii) *There exist functions $g, h\colon A^n \to B$ such that $f = g + h$, $h|_{A^n_=} \equiv 0$, $h \not\equiv 0$, and $\operatorname{ess} g = n - p$.*

The decomposition $f = g + h$ given above is unique.

Theorems 1.7 and 1.8 lead to the following characterization of functions with arity gap at least 3. A similar description was proposed by Shtrakov and Koppitz [9].

Corollary 1.9. *Assume that $(B;+)$ is a group with neutral element 0. Let $f\colon A^n \to B$, $n \geq 3$, and $3 \leq p \leq n$. Then the following two conditions are equivalent:*

(i) $\operatorname{ess} f = n$ *and* $\operatorname{gap} f = p$.

(ii) *There exist functions $g, h\colon A^n \to B$ such that $f = g + h$, $h|_{A^n_=} \equiv 0$, $h \not\equiv 0$, and $\operatorname{ess} g = n - p$.*

The decomposition $f = g + h$ given above is unique.

Analogous decompositions $f = g+h$ were presented in [5] for functions $f\colon A^n \to B$ with $\operatorname{gap} f = 2$ as well, in which either $\operatorname{ess} g = n - 2$ or g is a sum of essentially at most $(n-2)$-ary functions.

Having the previous results as our starting point, we present in the current paper yet another refinement of Theorem 1.7. Namely, we study the arity gap of polynomial functions over arbitrary fields. We will obtain further, more explicit decomposition schemes.

2. Arity gap of polynomial functions over fields

In what follows, we will assume that the reader is familiar with the basic notions of algebra, such as rings, unique factorization domains, fields, vector spaces, polynomials and polynomial functions. However, we find it useful to recall the following well-known result.

Fact 2.1. *Every function $f\colon F^n \to F$ on a finite field F is a polynomial function over F.*

Fact 2.1 establishes a correspondence between polynomials and functions over finite fields. This correspondence can be made bijective by assuming that we only consider polynomials over a given finite field, say $F = \mathrm{GF}(q)$, in which every exponent of every variable in every monomial is at most $q - 1$. This convention allows us to make no distinction between polynomials and their induced polynomial functions. Also, it is easy to verify that a given variable x_i is essential in a function induced by a polynomial $p \in F[x_1, \ldots, x_n]$ if and only if x_i occurs in p. Hence, in light of Remark 1.2, we may confine ourselves to considering only those polynomials in $F[x_1, \ldots, x_n]$ in which all variables occur.

We now recall the notion of partial derivative in the case of polynomial functions. The *partial derivative* of $f \in F[x_1, \ldots, x_n]$ with respect to its i-th variable is denoted by $\partial_i f$. The i-th partial derivative of a monomial is defined by the rule

$$\partial_i c x_1^{a_1} \cdots x_n^{a_n} = c a_i x_1^{a_1} \cdots x_{i-1}^{a_{i-1}} x_i^{a_i - 1} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n}. \tag{2}$$

Moreover, partial derivatives are additive, i.e.,

$$\partial_i \sum_{j \in J} f_j = \sum_{j \in J} \partial_i f_j. \tag{3}$$

The partial derivatives of arbitrary polynomial functions can then be determined by application of (2) and (3). Observe that for fields of characteristic 0, $\partial_i f = 0$ if and only if the i-th variable is inessential in f. Also, let us note the difference between

$$\partial_1 f(x_1, x_1, x_2) = \partial_1(f(x_1, x_1, x_2)) \quad \text{and} \quad (\partial_1 f)(x_1, x_1, x_2),$$

where $f \in F[x_1, x_2, x_3]$. The first one is a partial derivative of an identification minor of f, while the second one is an identification minor of a partial derivative of f. The chain rule gives the following relationship between these polynomials:

$$\partial_1 f(x_1, x_1, x_2) = (\partial_1 f)(x_1, x_1, x_2) + (\partial_2 f)(x_1, x_1, x_2).$$

Since we will often consider derivatives of simple minors, it is worth formulating a generalization of the above formula.

Fact 2.2. *Let $f \in F[x_1, \dots, x_n]$, $\sigma\colon [n] \to [m]$, and let $g \in F[x_1, \dots, x_m]$ be the simple minor of f defined by $g(x_1, \dots, x_m) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. Then the j-th partial derivative of g is*

$$\partial_j g = \sum_{\sigma(i)=j} (\partial_i f)(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Let F be a field, and let us apply the results of Section 1 in the case $A = B = F$ for polynomial functions $f \in F[x_1, \dots, x_n]$.

Lemma 2.3. *If f is a polynomial function over F, then the functions g and h in the decomposition $f = g + h$ given in Corollary 1.9 are also polynomial functions.*

Proof. Since $\operatorname{ess} g = n - p \leq n - 3$, the function g has at least three inessential variables, say the i-th and j-th variables are inessential in g. As $h|_{A^n_{\neq}} \equiv 0$, we have

$$f_{i \leftarrow j} = g_{i \leftarrow j} + h_{i \leftarrow j} = g + 0 = g.$$

Thus, g is a simple minor of f and hence a polynomial function. Then $h = f - g$ is a polynomial function as well. □

Lemma 2.4. *If h is an n-ary polynomial over F, then $h|_{F^n_{\neq}} \equiv 0$ if and only if h is a multiple of the polynomial*

$$\Delta(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Proof. It is clear that if h is multiple of Δ, then $h|_{F^n_{\neq}} \equiv 0$. Conversely, let us suppose that $h|_{F^n_{\neq}} \equiv 0$, and let us consider h as an element of $R[x_n]$, where R denotes the ring $F[x_1, \dots, x_{n-1}]$. Since $h|_{F^n_{\neq}} \equiv 0$, each one of the elements $x_1, \dots, x_{n-1} \in R$ are roots of the unary polynomial $h(x_n) \in R[x_n]$. Therefore h is divisible by $x_i - x_n$ for all $i = 1, \dots, n-1$. Repeating this argument with x_j in place of x_n, we can see that $x_i - x_j$ divides h for all $1 \leq i < j \leq n$. Since these divisors of h are relatively prime (and $F[x_1, \dots, x_n]$ is a unique factorization domain), we can conclude that h is divisible by their product. □

Combining the previous two lemmas with Corollary 1.9, we obtain the following description of polynomial functions over F with arity gap at least 3.

Theorem 2.5. *Let F be a field and let $f \in F[x_1, \dots, x_n]$ be a polynomial of arity at least 4. Then $\operatorname{gap} f = p \geq 3$ if and only if there exist polynomials $g, h \in F[x_1, \dots, x_n]$ such that $f = g + h$, exactly $n - p$ variables appear in g, and h is a nonzero multiple of the polynomial $\Delta(x_1, \dots, x_n)$. Moreover, the decomposition $f = g + h$ is unique.*

We consider the case $\operatorname{gap} f = 2$ in the next section, and we will see that in this case a nice decomposition of polynomial functions over a finite field F can be given if and only if F has characteristic 2. Polynomials over fields of characteristic 0 are dealt with in Section 4; the case of infinite fields of finite characteristic is left open.

3. Arity gap of polynomial functions over finite fields of characteristic 2

The following proposition refines Fact 1.6 for polynomial functions over finite fields of characteristic 2.

Proposition 3.1. *Let $F := \mathrm{GF}(q)$, where q is a power of 2, and let $f \in F[x_1, \dots, x_n]$. Then f is determined by* oddsupp *if and only if*

(A) *f is symmetric, i.e., the coefficients of $x_1^{k_1} \cdots x_n^{k_n}$ and $x_1^{l_1} \cdots x_n^{l_n}$ are the same whenever there is a permutation $\pi \in S_n$ such that $k_i = l_{\pi(i)}$ for all $i \in [n]$, and*

(B) *the coefficient of $x_1^{k_1} \cdots x_n^{k_n}$ is 0 whenever there exist $i \neq j$ such that $k_i = k_j \neq 0$.*

Proof. Let U be the set of polynomials $f \in F[x_1, \dots, x_n]$ that are determined by oddsupp, and let V be the set of polynomials $f \in F[x_1, \dots, x_n]$ satisfying conditions (A) and (B). Then both U and V are finite-dimensional vector spaces over F.

We claim that $V \subseteq U$. If $f \in V$, then f is totally symmetric by condition (A). To see that f is determined by oddsupp, by Fact 1.6, it suffices to verify that $f_{2 \leftarrow 1}$ does not depend on x_1. Let us consider an arbitrary monomial $M := c x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ of f, in which at least one of x_1 and x_2 appears with a non-zero exponent. By condition (A), the monomial $M' := c x_1^{k_2} x_2^{k_1} \cdots x_n^{k_n}$ appears in f as well, and from condition (B) it follows that $M \neq M'$. Identifying x_1 and x_2, the monomials M and M' will cancel each other, since the characteristic of F is 2. This shows that x_1 does not appear in $f_{2 \leftarrow 1}$; hence $f \in U$.

Therefore, in order to prove that $U = V$, it suffices to show that $\dim U = \dim V$. The dimension of U equals the cardinality of the set $\mathcal{P}'_n(F)$, which is 2^{q-1} if $n \geq q$, and

$$\binom{q}{n} + \binom{q}{n-2} + \binom{q}{n-4} + \cdots$$

if $n < q$. The dimension of V is 2^{q-1} if $n \geq q$ and

$$\binom{q-1}{n} + \binom{q-1}{n-1} + \binom{q-1}{n-2} + \cdots$$

if $n < q$. Thus the proposition boils down to the identity

$$\binom{q}{n} + \binom{q}{n-2} + \binom{q}{n-4} + \cdots = \binom{q-1}{n} + \binom{q-1}{n-1} + \binom{q-1}{n-2} + \cdots,$$

which is not difficult to verify using the identity

$$\binom{m}{t} = \binom{m-1}{t} + \binom{m-1}{t-1}. \qquad \square$$

Proposition 3.2. *Let $F := \mathrm{GF}(q)$, where q is a power of 2, and let $f \in F[x_1, \dots, x_n]$. Then $f|_{F^n_=}$ is determined by* oddsupp *if and only if there exist polynomials $g, h \in F[x_1, \dots, x_n]$ such that $f = g + h$, conditions* (A) *and* (B) *are satisfied by g, and h is a multiple of the polynomial $\Delta(x_1, \dots, x_n)$.*

Proof. For sufficiency, let us assume that $f = g + h$, where g and h are as in the statement of the proposition. It follows from Proposition 3.1 that g is determined by oddsupp; hence $g|_{F^n_=}$ is determined by oddsupp. Moreover, $h|_{F^n_=} \equiv 0$ by Lemma 2.4. Thus, $f|_{F^n_=} = g|_{F^n_=} + h|_{F^n_=} = g|_{F^n_=}$ is determined by oddsupp as well.

For necessity, if $f|_{F^n_=}$ is determined by oddsupp, then there is a (not necessarily unique) function g such that g is determined by oddsupp and $f|_{F^n_=} = g|_{F^n_=}$. By Fact 2.1, g is a polynomial function; hence so is $h = f - g$. Now we apply Proposition 3.1 to g, and Lemma 2.4 to h. $\square$

Theorem 3.3. *Let $F := \mathrm{GF}(q)$, where q is a power of 2, and let $f \in F[x_1, \dots, x_n]$ be a polynomial of arity at least 4 which depends on all of its variables. Then $\operatorname{gap} f = p \geq 2$ if and only if there exist polynomials $g, h \in F[x_1, \dots, x_n]$ such that $f = g + h$, h is multiple of the polynomial $\Delta(x_1, \dots, x_n)$, and either*

(a) *exactly $n - p$ variables appear in g and $h \neq 0$, or*
(b) *g is not constant and satisfies conditions* (A) *and* (B).

Otherwise $\operatorname{gap} f = 1$.

Proof. Combine Theorem 1.7, Theorem 1.8, Lemma 2.4 and Proposition 3.2, and observe that if $f|_{F^n_=}$ is determined by oddsupp then $\operatorname{qa} f = n$ if and only if $f|_{F^n_=}$ is not constant. $\square$

Corollary 3.4. *Let $F = \mathrm{GF}(q)$, where q is a power of 2, and let $f \in F[x_1, \dots, x_n]$ be a polynomial of essential arity $n > \max(q, 3)$. If $\operatorname{gap} f = 2$, then f can be decomposed into a sum of essentially at most $(q-1)$-ary functions.*

Proof. If $n > q$, then $F^n_= = F^n$; hence case (a) in Theorem 3.3 cannot occur, while in case (b) we have $h \equiv 0$; thus $f = g$. Moreover, in case (b), every monomial of g involves at most $q - 1$ variables, by condition (B). This implies that f can be written as a sum of essentially at most $(q-1)$-ary functions, namely the polynomial functions corresponding to the monomials of f. $\square$

Remark 3.5. The decomposition given in Theorem 3.3 is unique only in case (a). In case (b) it can be made unique by requiring that g is constant 0 on $F \setminus F^n_=$.

Remark 3.6. Applying Corollary 3.4 in the case $q = 2$, we see that any function $f\colon \{0,1\}^n \to \{0,1\}$ with essential arity $n \geq 4$ and $\operatorname{gap} f = 2$ can be written as a sum of at most unary functions, i.e., that f is a linear function (cf. Example 1.4 and [2]).

Remark 3.7. From the results of [5] it follows that if A is a finite set and B is a Boolean group, then every function $f\colon A^n \to B$ with essential arity $n > \max(|A|, 3)$ and $\operatorname{gap} f = 2$ can be decomposed into a sum of essentially at most $(n-2)$-ary functions. Corollary 3.4 shows that the bound $n - 2$ on the essential arity of the

summands can be improved to $q-1$ (which is independent of n) if $A = B = \mathrm{GF}(q)$, where q is a power of 2 (for further results in this direction see also [7]). In the example below, we will construct a polynomial $f \in F[x_1, \dots, x_n]$ over $\mathrm{GF}(q)$ for any odd prime power q and any $n \geq 2$, such that $\operatorname{gap} f = 2$ but f cannot be written as a sum of $(n-1)$-ary functions. This shows that Corollary 3.4 does not hold for finite fields with odd characteristic and that the condition of B's being a Boolean group cannot be dropped in the aforementioned result of [5].

Example 3.8. Let q be an odd prime power, and let f be the polynomial function

$$f(x_1, \dots, x_n) = \prod_{i=1}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big)$$

over $\mathrm{GF}(q)$, where $\frac{1}{2}$ stands for the multiplicative inverse of $2 = 1 + 1$ (it exists, since $\mathrm{GF}(q)$ is of odd characteristic). Let us identify the first two variables of f:

$$\begin{aligned} f(x_1, x_1, x_3, \dots, x_n) &= \Big(x_1^{q-1} - \frac{1}{2} \Big)^2 \cdot \prod_{i=3}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big) \\ &= \Big(x_1^{2q-2} - x_1^{q-1} + \frac{1}{4} \Big) \cdot \prod_{i=3}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big) \\ &= \frac{1}{4} \cdot \prod_{i=3}^{n} \Big(x_i^{q-1} - \frac{1}{2} \Big), \end{aligned}$$

since $x_1^q = x_1$ holds identically in f. We see that x_1 becomes an inessential variable, and $\operatorname{ess} f_{2 \leftarrow 1} = n - 2$. This together with the total symmetry of f shows that $\operatorname{gap} f = 2$.

Suppose that f is a sum of at most $(n-1)$-ary functions. By Fact 2.1, these functions can be written as polynomials. This implies that every monomial of f involves at most $n-1$ variables. However, this is clearly not the case, as the expansion of f involves the monomial $x_1^{q-1} \cdots x_n^{q-1}$, which will not be cancelled by any other monomial. This contradiction shows that f cannot be expressed as a sum of at most $(n-1)$-ary functions.

4. Arity gap of polynomial functions over fields of characteristic 0

We now consider the case of polynomial functions over fields of characteristic 0. Unlike polynomials over fields of characteristic 2 (see Proposition 3.2), it turns out that in the current case there is no polynomial function $f \colon F^n \to F$ whose restriction $f|_{F^n_{\neq}}$ is nonconstant and determined by oddsupp.

Lemma 4.1. *Let F be a field of characteristic 0 and let $f \in F[x_1, \dots, x_n]$ be a polynomial of arity at least 2. If $f|_{F^n_{\neq}}$ is determined by* oddsupp*, then $f|_{F^n_{\neq}}$ is constant, i.e.,* $\operatorname{qa} f = 0$.

Proof. For $n = 2$, the claim is trivial, so we will assume that $n \geq 3$. Let us suppose that $f|_{F^n_{\neq}}$ is determined by oddsupp. Then $f(x_1, x_1, x_3, \dots, x_n)$ does not depend on x_1 by Fact 1.6; hence we have

$$(\partial_1 f)(x_1, x_1, x_3, \dots, x_n) + (\partial_2 f)(x_1, x_1, x_3, \dots, x_n) = 0$$

by Fact 2.2. Let $\mathbf{u} = (x_1, x_1, x_1, x_4, \dots, x_n) \in F^n$. From the above equality it follows that

$$(\partial_1 f)(\mathbf{u}) + (\partial_2 f)(\mathbf{u}) = 0,$$

and a similar argument shows that

$$(\partial_1 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u}) = 0 \quad \text{and} \quad (\partial_2 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u}) = 0.$$

Since the characteristic of F is different from 2, by adding these three equalities we can conclude that

$$(\partial_1 f)(\mathbf{u}) + (\partial_2 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u}) = 0.$$

However, according to Fact 2.2, $(\partial_1 f)(\mathbf{u}) + (\partial_2 f)(\mathbf{u}) + (\partial_3 f)(\mathbf{u})$ is nothing else but the derivative of $f(x_1, x_1, x_1, x_4, \dots, x_n)$ with respect to x_1. This implies that $f(x_1, x_1, x_1, x_4, \dots, x_n)$ does not depend on x_1, i.e.,

$$f(a, a, a, x_4, \dots, x_n) = f(b, b, b, x_4, \dots, x_n) \tag{4}$$

for any $a, b, x_4, \dots, x_n \in F$.

Informally, equality (4) means that whenever the first three entries of an n-tuple are the same, then replacing these three entries with another element of F, the value of f does not change. (By symmetry, this is certainly true for any three entries, not only the first three.) From the definition of being determined by oddsupp it follows immediately that we can also change any two identical entries:

$$f(\cdots a \cdots a \cdots) = f(\cdots b \cdots b \cdots). \tag{5}$$

Let $\mathbf{x} = (x_1, \dots, x_n)$ be any vector in $F^n_{=}$. We may suppose without loss of generality that $x_1 = x_2$. With the help of (4) and (5) we can replace the entries of $\mathbf{x}$ in triples and pairs, until all of them are the same:

$$\begin{aligned} f(\mathbf{x}) &= f(\underline{x_1, x_1}, x_3, x_4, x_5, x_6, \dots, x_n) \\ &= f(\underline{x_3, x_3, x_3}, x_4, x_5, x_6, \dots, x_n) \\ &= f(\underline{x_4, x_4}, \underline{x_4, x_4}, x_5, x_6, \dots, x_n) \\ &= f(\underline{x_5, x_5, x_5}, \underline{x_5, x_5}, x_6, \dots, x_n) \\ &= f(\underline{x_6, x_6}, \underline{x_6, x_6}, \underline{x_6, x_6}, \dots, x_n) = \cdots \\ &= f(x_n, x_n, x_n, x_n, x_n, x_n, \dots, x_n). \end{aligned}$$

If n is even, then (5) shows that $f(\mathbf{x}) = f(\mathbf{0})$:

$$f(\mathbf{x}) = f(\underline{x_n, x_n}, \underline{x_n, x_n}, \dots, \underline{x_n, x_n}) = f(0, 0, 0, 0, \dots, 0, 0);$$

while if n is odd, then we use both (4) and (5):

$$f(\mathbf{x}) = f(\underline{x_n, x_n, x_n}, \underline{x_n, x_n}, \dots, \underline{x_n, x_n}) = f(0, 0, 0, 0, 0, \dots, 0, 0).$$

We have shown that $f(\mathbf{x}) = f(\mathbf{0})$ for all $\mathbf{x} \in F^n_{=}$; hence $f|_{F^n_{=}}$ is indeed constant. □

Lemma 4.2. *Let F be a field of characteristic 0 and let $f \in F[x_1, x_2, x_3]$. If* $\operatorname{gap} f = 2$*, then* $\operatorname{qa} f = 1$.

Proof. By case (iii) of Theorem 1.7, there exist a nonconstant map $h\colon A \to B$ and $i_1, i_2, i_3 \in \{0, 1\}$ such that

$$\begin{aligned} f(x_1, x_0, x_0) &= h(x_{i_1}), \\ f(x_0, x_1, x_0) &= h(x_{i_2}), \\ f(x_0, x_0, x_1) &= h(x_{i_3}). \end{aligned}$$

Up to permutation of variables there are four possibilities for (i_1, i_2, i_3), namely $(1, 1, 1)$, $(0, 0, 0)$, $(1, 1, 0)$ and $(1, 0, 0)$. We will show that the first three cases cannot occur.

If $(i_1, i_2, i_3) = (1, 1, 1)$ then f is determined by oddsupp, and then Lemma 4.1 shows that h is constant, a contradiction.

If $(i_1, i_2, i_3) = (0, 0, 0)$ then $f(x_2, x_1, x_1) = f(x_1, x_2, x_1) = f(x_1, x_1, x_2) = h(x_1)$; hence $f(x_2, x_1, x_1)$ does not depend on x_2. By Fact 2.2 this means that $(\partial_1 f)(x_2, x_1, x_1) = 0$, in particular, $(\partial_1 f)(x_1, x_1, x_1) = 0$ for all $x_1 \in F$. Similarly, we have $(\partial_2 f)(x_1, x_1, x_1) = (\partial_3 f)(x_1, x_1, x_1) = 0$. Another application of Fact 2.2 yields

$$\begin{aligned}\partial_1 h(x_1) &= \partial_1 f(x_1, x_1, x_1) \\ &= (\partial_1 f)(x_1, x_1, x_1) + (\partial_2 f)(x_1, x_1, x_1) + (\partial_3 f)(x_1, x_1, x_1) = 0,\end{aligned}$$

and this means that h is constant, a contradiction.

If $(i_1, i_2, i_3) = (1, 1, 0)$, then $f(x_1, x_2, x_2) = f(x_2, x_1, x_2) = f(x_1, x_1, x_2) = h(x_1)$, which does not depend on x_2. Again, by Fact 2.2 we see that

$$\begin{aligned}(\partial_2 f)(x_1, x_2, x_2) + (\partial_3 f)(x_1, x_2, x_2) &= 0, \\ (\partial_1 f)(x_2, x_1, x_2) + (\partial_3 f)(x_2, x_1, x_2) &= 0, \\ (\partial_3 f)(x_1, x_1, x_2) &= 0.\end{aligned}$$

From these equalities it follows that

$$(\partial_1 f)(x_1, x_1, x_1) = (\partial_2 f)(x_1, x_1, x_1) = (\partial_3 f)(x_1, x_1, x_1) = 0,$$

which is again a contradiction.

We are left with the case that $(i_1, i_2, i_3) = (1, 0, 0)$ (up to permutation). This implies that $f|_{F^3_{\neq}} = h(x_1)|_{F^3_{\neq}}$, i.e., $\operatorname{qa} f = 1$. □

Theorem 4.3. *Let F be a field of characteristic 0 and let $f \in F[x_1, \dots, x_n]$ be a polynomial of arity at least 2 that depends on all of its variables. Then $\operatorname{gap} f = p \geq 2$ if and only if there exist polynomials $g, h \in F[x_1, \dots, x_n]$ such that $f = g + h$, exactly $n - p$ variables appear in g, and h is a nonzero multiple of the polynomial $\Delta(x_1, \dots, x_n)$. Otherwise $\operatorname{gap} f = 1$. Moreover, the decomposition $f = g + h$ is unique.*

Proof. For necessity, assume that $\operatorname{gap} f = p \geq 2$. By Lemma 4.1, if $f|_{F^n_{\neq}}$ is determined by oddsupp, then $\operatorname{qa} f = 0$. Theorem 1.7 and Lemma 4.2 then imply that if $\operatorname{gap} f = p \geq 2$, then $\operatorname{qa} f = n - p$. By Theorem 1.8, there exist unique functions $g, h \colon A^n \to B$ such that $f = g + h$, $h|_{F^n_{\neq}} \equiv 0$, $h \not\equiv 0$ and $\operatorname{ess} g = n - p$. By Lemma 2.4, h is a multiple of $\Delta(x_1, \dots, x_n)$.

For sufficiency, assume that $f = g + h$, where g and h are as in the statement of the theorem. Then $\operatorname{ess} g = n - p$, $h \not\equiv 0$ and $h|_{F^n_{\neq}} \equiv 0$ by Lemma 2.4. From Theorem 1.8 it follows that $\operatorname{qa} f = n - p$, and then Theorem 1.7 implies that $\operatorname{gap} f = p$. □

Let us note that in the proof of the above theorem we did not really make use of the fact that f is a polynomial; we only used the basic properties of the derivative. Therefore the theorem remains valid for differentiable real functions.

Theorem 4.4. *Let $f \colon \mathbb{R}^n \to \mathbb{R}$ be a differentiable function of arity at least 2. Then $\operatorname{gap} f = p \geq 2$ if and only if there exist differentiable functions $g, h \colon \mathbb{R}^n \to \mathbb{R}$ such that $f = g + h$, $h|_{\mathbb{R}^n_{\neq}} \equiv 0$, $h \not\equiv 0$, and $\operatorname{ess} g = n - p$. Otherwise $\operatorname{gap} f = 1$. Moreover, the decomposition $f = g + h$ is unique.*

Acknowledgments

The third named author acknowledges that the present project is supported by the TÁMOP-4.2.1/B-09/1/KONV-2010-0005 program of National Development Agency of Hungary, by the Hungarian National Foundation for Scientific Research under grants no. K77409 and K83219, by the National Research Fund of Luxembourg, and cofunded under the Marie Curie Actions of the European Commission (FP7-COFUND).

References

[1] J. Berman, A. Kisielewicz, On the number of operations in a clone, *Proc. Amer. Math. Soc.* **122** (1994) 359–369.

[2] M. Couceiro, E. Lehtonen, On the effect of variable identification on the essential arity of functions on finite sets, *Int. J. Found. Comput. Sci.* **18** (2007) 975–986.

[3] M. Couceiro, E. Lehtonen, Generalizations of Świerczkowski's lemma and the arity gap of finite functions, *Discrete Math.* **309** (2009) 5905–5912.

[4] M. Couceiro, E. Lehtonen, The arity gap of polynomial functions over bounded distributive lattices, *40th IEEE International Symposium on Multiple-Valued Logic (ISMVL 2010),* IEEE Computer Society, Los Alamitos, 2010, pp. 113–116.

[5] M. Couceiro, E. Lehtonen, T. Waldhauser, Decompositions of functions based on arity gap, arXiv:1003.1294.

[6] M. Couceiro, E. Lehtonen, T. Waldhauser, The arity gap of aggregation functions and further extensions, arXiv:1003.2192.

[7] M. Couceiro, E. Lehtonen, T. Waldhauser, Additive decomposability of functions over Abelian groups, manuscript.

[8] A. Salomaa, On essential variables of functions, especially in the algebra of logic, *Ann. Acad. Sci. Fenn. Ser. A I. Math.* **339** (1963) 3–11.

[9] S. Shtrakov, J. Koppitz, On finite functions with non-trivial arity gap, *Discuss. Math. Gen. Algebra Appl.* **30** (2010) 217–245.

[10] R. Willard, Essential arities of term operations in finite algebras, *Discrete Math.* **149** (1996) 239–259.

(M. Couceiro) Mathematics Research Unit, University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: miguel.couceiro@uni.lu

(E. Lehtonen) Computer Science and Communications Research Unit, University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: erkko.lehtonen@uni.lu

(T. Waldhauser) Mathematics Research Unit, University of Luxembourg, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg and Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary

E-mail address: twaldha@math.u-szeged.hu